Apéndice de la documentación

Software de seguridad de Zone Alarm versión 7.1

En este documento se presentan nuevas funciones que no se incluyeron en las versiones traducidas de la guía del usuario. Si desea obtener más información sobre cualquier elemento de la lista, haga clic en él.

- **Centro de protección de identidad de ZoneAlarm**: Le permitirá evitar y detectar los robos de identidad y, si es necesario, recuperarse de ellos.
- **Modo de juego**: Suprime temporalmente la mayor parte de los análisis, actualizaciones de productos y alertas del software de seguridad de Zone Alarm, lo que le permitirá disfrutar de los juegos en su equipo sin apenas interrupciones.
- **Protecciones especiales del sistema de OSFirewall**: Determina si los programas de su equipo pueden realizar acciones específicas como modificar la página de inicio de Internet Explorer o instalar controles ActiveX.
- **Opciones de análisis de virus**: Ofrece la posibilidad de omitir el análisis de archivos de tamaño superior al especificado y proporciona una base de datos de software maligno ampliada.
- **Análisis de la memoria del sistema**: Analiza la memoria RAM del equipo.
- **Lista de excepciones**: Ofrece la posibilidad de administrar una lista de elementos que desea que se ignoren en los análisis de virus realizados por el software de seguridad de Zone Alarm.
- **Nivel de control de programas**: Proporciona un modo de aprendizaje automático que minimiza las alertas de programas mientras el software de seguridad de Zone Alarm se familiariza con el contenido de su equipo.
- **Configuración de las opciones de seguridad de red**: Ofrece la posibilidad de permitir o bloquear el tráfico de Internet que utiliza Internet Protocol versión 6 (IPv6).
- **Actualizaciones y correcciones de documentación**

Centro de protección de identidad de ZoneAlarm

Con la proliferación del comercio electrónico, el mantenimiento de registros electrónicos y los correos financieros masivos, la incidencia de los robos de identidad ha aumentado en los últimos años. Los piratas informáticos pueden utilizar software maligno para interceptar su información personal en línea. Además, pueden robar sus CD y equipos portátiles con información de clientes y pueden interceptar correos confidenciales (como ofertas de tarjetas de crédito aprobadas previamente) con información personal.

El Centro de protección de identidad de ZoneAlarm es un sitio Web que le ayudará a evitar y detectar los robos de identidad y, si es necesario, recuperarse de ellos. El Centro de protección de identidad ofrece consejos para proteger su identidad, así como recursos para controlar el uso de su información personal y recuperarse de los robos de identidad.

Puede acceder al Centro de protección de identidad a través de ZoneAlarm Pro y ZoneAlarm Security Suite.

Para visitar el Centro de protección de identidad:

1. Vaya a **Protección de identidad | Principal**.
2. En el área Centro de protección de identidad, haga clic en **Ir al Centro de protección de identidad de ZoneAlarm**.

Modo de juego

El modo de juego suprime temporalmente la mayor parte de los análisis, actualizaciones de productos y alertas del software de seguridad de Zone Alarm, lo que le permitirá disfrutar de los juegos en su equipo sin apenas interrupciones. En modo de juego, podrá permitir o denegar las solicitudes de permiso de todos los programas, de modo que el software de seguridad de Zone Alarm podrá responder a dichas solicitudes automáticamente sin mostrar alertas. Los análisis automáticos y las actualizaciones de productos se pospondrán hasta que se desactive el modo de juego. El modo de juego seguirá activo hasta que lo desactive o hasta que cierre el software de seguridad de Zone Alarm o apague el equipo.

El modo de juego suprimirá todas las alertas informativas y todas las alertas en las que deba tomar una decisión. Esto incluye las alertas originadas por la opción Preguntar de la lista de programas, como las alertas de permiso activadas por programas que intentan enviar correo o actuar como servidores. También incluye las alertas de OSFirewall que le preguntan si desea permitir o denegar un comportamiento inusual o sospechoso. El modo de juego no anula las opciones Bloquear o Permitir de la lista de programas. Si ha configurado el software de seguridad de Zone Alarm para que bloquee siempre un programa determinado, seguirá bloqueando dicho programa aunque active el modo de juego con la opción Permitir.

El uso del modo de juego puede reducir la seguridad del sistema. Si decide permitir todas las solicitudes de permiso, pueden aumentar las posibilidades de que un

programa maligno dañe su equipo o acceda a sus datos. Por otro lado, si decide denegar todas las solicitudes, puede interrumpir las funciones de los programas legítimos. Por tanto, únicamente deberá activar el modo de juego mientras esté jugando.

Para activar el modo de juego:

1. Haga clic con el botón derecho en el icono de la barra de tareas y elija **Modo de juego...**
2. En el cuadro de diálogo Activar modo de juego, haga clic en una de las siguientes opciones:

   Responder a todas las alertas con "Permitir"—Se dará permiso a todas las solicitudes.

   Responder a todas las alertas con "Denegar"—Se denegará el permiso a todas las solicitudes.
3. Deje el cuadro de diálogo Activar modo de juego abierto o minimícelo, pero no lo cierre. (Si cierra la ventana, desactivará el modo de juego.)

   Mientras el modo de juego esté activo, el software de seguridad de Zone Alarm mostrará el icono especial en la barra de tareas.

Para desactivar el modo de juego:

Realice una de las siguientes acciones:

- Haga clic en **Cancelar** o en el icono de cierre (x) situado en la esquina superior derecha para cerrar el cuadro de diálogo Activar modo de juego.
- Haga clic en **Detener modo de juego** en el cuadro de diálogo Activar modo de juego.
- Haga clic con el botón derecho en el icono de la barra de tareas y seleccione **Detener modo de juego**.

Tenga en cuenta que el modo de juego se desactivará automáticamente si apaga el equipo o cierra el software de seguridad de Zone Alarm.

Protecciones especiales del sistema de OSFirewall

La protección de OSFirewall, activada de forma predeterminada, detecta si un programa está intentando utilizar su sistema operativo para realizar acciones sospechosas en su equipo. También podrá configurar las protecciones especiales del sistema de OSFirewall, que determinan si los programas instalados en su equipo

pueden realizar determinadas acciones como modificar la página de inicio de Internet Explorer o instalar controles ActiveX.

Las protecciones especiales del sistema de OSFirewall pueden evitar algunos de los comportamientos sospechosos de nivel medio tratados en el apéndice "Actividades de programas".

Para configurar OSFirewall:

1. Seleccione **Control de programas|Principal**.
2. En el área Control de programas, haga clic en **Personalizar**.
3. En el cuadro de diálogo Configuración personalizada de control de programas, seleccione la ficha **OSFirewall**.
4. Seleccione o cancele la selección de **Activar OSFirewall**, según prefiera. (Tenga en cuenta que para configurar las protecciones especiales del sistema de OSFirewall en el paso siguiente, debe seleccionar antes esta casilla de verificación.)
5. Configure las protecciones especiales del sistema de OSFirewall que prefiera. En cada acción de la lista, haga clic en el campo Estado y seleccione **Permitir**, **Denegar**, **Preguntar** o **Utilizar configuración del programa**. Si selecciona Utilizar configuración del programa, el software de seguridad de Zone Labs consultará la configuración de SmartDefense Advisor o la configuración manual establecida por el usuario.
6. Haga clic en **Aplicar** para guardar la configuración y dejar el cuadro de diálogo abierto o en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo.

Opciones de análisis de virus

Puede configurar su análisis de virus para que ignore cualquier archivo cuyo tamaño sea superior al especificado (el valor predeterminado es 8 MB). Esta opción mejora el tiempo de análisis sin aumentar el riesgo, ya que los archivos de virus suelen ser menores de 8 MB. Aunque los archivos grandes ignorados en el análisis puedan contener virus, su equipo seguirá estando protegido si tiene activada la opción de análisis al obtener acceso.

También puede activar la base de datos ampliada. Esta base de datos incluye una lista completa de software maligno además de la lista de virus estándar. Sin embargo, hay software maligno incluido en la base de datos ampliada que también puede aparecer en la base de datos de programas informáticos espía estándar, y hay software maligno sospechoso que se puede analizar dos veces. La lista de software maligno de la base de datos ampliada puede incluir programas que se consideran inofensivos.

Para especificar opciones de análisis de virus:

1. Seleccione **Antivirus / Protección contra programas informáticos espía|Principal** y, a continuación, haga clic en **Opciones avanzadas**.

   Aparecerá el cuadro de diálogo Opciones avanzadas.

2. En **Gestión de virus**, seleccione **Opciones de análisis**.

3. Active o desactive la casilla de verificación **Omitir si el objeto es superior a**.

   Si ha activado esta casilla de verificación, introduzca un tamaño de objeto máximo en el campo **MB**.

4. Active o desactive la casilla de verificación **Activar base de datos ampliada** y a continuación, haga clic en **Aceptar**.

Análisis de la memoria del sistema

Para analizar la memoria del sistema, realice los siguientes pasos.

Para analizar la memoria del sistema:

1. Seleccione **Antivirus / Protección contra programas informáticos espía|Principal**.

2. Haga clic en **Opciones avanzadas**.

   Aparecerá el cuadro de diálogo Opciones avanzadas.

3. En Gestión de virus, seleccione **Destinos de análisis**.

4. Seleccione las unidades, las carpetas y los archivos que desee analizar.

5. Active o desactive la casilla de verificación **Analizar los sectores de arranque de todas las unidades locales**.

6. Active o desactive la casilla de verificación de **análisis de la memoria del sistema** y haga clic en **Aceptar**.

Lista de excepciones

Aunque algunos programas considerados sospechosos por la base de datos ampliada pueden ser potencialmente dañinos para su equipo o hacer que sus datos sean vulnerables a ataques de piratas informáticos, hay muchas aplicaciones potencialmente inofensivas que se detectan como virus durante un análisis. Si utiliza algunas de estas aplicaciones, puede agregarla a la lista de excepciones para excluirla de los análisis antivirus. Para agregar programas a la lista de excepciones, haga clic con el botón derecho en el elemento correspondiente de la lista Resultados del análisis y seleccione la opción de menú Ignorar siempre.

Una vez que se hayan incluido en la lista de excepciones, los programas no volverán a detectarse durante los análisis antivirus. Si se ha agregado un virus a la lista de excepciones por error, es posible eliminarlo manualmente.

Para eliminar virus de la lista de excepciones:

1. Seleccione **Antivirus / Protección contra programas informáticos espía|Principal** y, a continuación, haga clic en **Opciones avanzadas**.
2. En Gestión de virus, seleccione **Excepciones**.
3. En el área Excepciones de tratamiento de virus, seleccione el virus que desee eliminar y, a continuación, haga clic en **Eliminar de la lista**.
4. Haga clic en **Aceptar**.

Nivel de control de programas

El software de seguridad de Zone Alarm ofrece varios métodos de control de programas. El control de programas básico permite determinar los derechos de acceso y de servidor para programas individuales. El control avanzado de programas evita que el software maligno utilice incorrectamente los programas de confianza. El control de interacción de aplicación le avisa si hay algún proceso intentando utilizar otro proceso o si hay algún programa intentando iniciar otro programa. La protección de OSFirewall detecta si un programa está intentando utilizar su sistema operativo para realizar acciones sospechosas en su equipo.

Para limitar el número de alertas que verá, puede utilizar las funciones siguientes:

- Si utiliza el software de seguridad de Zone Alarm con antivirus, utilice el nivel de control de programas Aprendizaje automático. Aprendizaje automático proporciona un nivel de protección moderado durante los primeros 7 a 21 días de uso del software de seguridad de Zone Alarm. Una vez que el software de seguridad de Zone Alarm conozca su equipo, restablecerá el nivel de control de programas Máximo.
- Para aprovechar las ventajas de la configuración del programa recomendada de Zone Alarm, utilice SmartDefense Advisor junto con el control de programas.

Para establecer el nivel de control de programas:

1. Seleccione **Control de programas|Principal**.
2. En el área Control de programas, haga clic en el control deslizante y arrástrelo hasta la configuración que desee.

Máx. (para versiones con antivirus) Alto (para versiones sin antivirus)	Con esta configuración es posible que vea una gran cantidad de alertas. ◆ Los programas deberán solicitar acceso a Internet y derechos de servidor. ◆ OSFirewall buscará comportamientos sospechosos. ◆ El control avanzado de programas y el control de interacción de aplicación estarán activados. ◆ De forma predeterminada, el control de componentes estará desactivado.*

Automático (para versiones con antivirus)	Este modo minimiza el número de alertas. ◆ Este nivel de control es menos seguro entre los primeros 7 y 21 días. ◆ La red y OSFirewall examinarán algunos programas.
Medio (para versiones sin antivirus)	Ésta es la configuración predeterminada. ◆ Los programas deberán solicitar acceso a Internet y derechos de servidor. ◆ OSFirewall buscará comportamientos sospechosos. ◆ De forma predeterminada, el control de componentes estará desactivado.*
Mín. (para versiones con antivirus)	◆ OSFirewall estará desactivado. ◆ De forma predeterminada, el control de componentes estará desactivado.* ◆ Estarán disponibles el control de servidor y el modo invisible
Bajo (para versiones sin antivirus)	◆ OSFirewall estará desactivado. ◆ De forma predeterminada, el control de componentes estará desactivado.* ◆ No estarán disponibles el control de servidor ni el modo invisible
Desactivado	El control de programas estará desactivado. ◆ No se autenticarán ni reconocerán programas ni componentes. ◆ No se aplicarán permisos de programas. ◆ Todos los programas tendrán derechos de servidor/acceso. ◆ Todos los programas podrán realizar actividades sospechosas. ◆ No se mostrarán alertas de programas.

* El control de componentes estará desactivado de forma predeterminada. Si ha activado el control de componentes, éste permanecerá activado mientras que el control de programas esté establecido en Alto, Medio o Bajo.

Configuración de las opciones de seguridad de red

La detección automática de red permite configurar la zona de confianza fácilmente para que no se interrumpan las actividades normales de red local, como el uso compartido de archivos e impresoras. El software de seguridad de Zone Alarm detectará sólo las redes a las que esté conectado físicamente. Las conexiones de red enrutadas o virtuales no se pueden detectar.

Puede configurar el software de seguridad de Zone Alarm para que incluya automáticamente todas las redes detectadas en la zona de confianza o para que le pregunte antes de agregar nuevas redes detectadas.

Para especificar la configuración de red:

1. Seleccione **Servidor de seguridad**|**Principal**.
2. Haga clic en **Opciones avanzadas**.
3. En el área de configuración de red, seleccione las opciones de seguridad.

Incluir redes en zona de confianza al ser detectadas	Mueve automáticamente las redes nuevas a la zona de confianza. Ésta es la opción menos segura.
Excluir redes de zona de confianza al ser detectadas	No agrega las nuevas redes a la zona de confianza, sino que las coloca en la zona de Internet. Ésta es la opción más segura.
Preguntar en qué zona colocar nuevas redes al ser detectadas	El software de seguridad de Zone Alarm muestra una alerta de red nueva o el asistente para la configuración de red, que le permitirá especificar la zona.
Colocar automáticamente redes inalámbricas sin proteger (WEP o WPA) en la zona de Internet	Coloca las redes inalámbricas inseguras en la zona de Internet automáticamente, lo que evita que otros usuarios de la red puedan acceder sin autorización a sus datos.
Activar la red IPv6	Permite que el tráfico de la red IPv6 pueda acceder a su equipo.

Actualizaciones y correcciones de documentación

En la siguiente sección se incluyen actualizaciones y correcciones no incluidas en el cuerpo principal de la ayuda en línea o la guía del usuario de las versiones traducidas.

- "Análisis de programas espía", en la página 8
- "Exclusión de programas espía de los análisis", en la página 9
- "Resultados del análisis de virus y programas espía", en la página 9
- "Control de componentes", en la página 9
- "Nuevo comportamiento para Recordar esta configuración", en la página 10
- "Cambio de nombre en el panel Servidor de seguridad", en la página 10
- "Nuevos iconos de la barra de tareas", en la página 10

Análisis de programas espía

En versiones anteriores del software de seguridad de Zone Alarm, la documentación especificaba que se podía iniciar una análisis de programas espía abriendo el archivo o haciendo clic con el botón derecho en un archivo y seleccionando la opción de análisis. Esto es incorrecto.

Existen dos formas de iniciar un análisis de programas espía:

- Puede hacer clic en **Buscar programas espía** en el área Protección contra programas informáticos espía de la ficha Principal del panel **Antivirus / Protección contra programas informáticos espía**.
- Puede programar que se ejecute un análisis del sistema una vez o a intervalos regulares. (Si desea obtener información detallada sobre cómo configurar esta opción, consulte la ayuda en línea asociada.)

Exclusión de programas espía de los análisis

En versiones anteriores de la documentación, las indicaciones para excluir determinados programas de los análisis omitían algunos detalles. A continuación se incluye el texto corregido:

Aunque algunos programas espía pueden ser potencialmente dañinos para su equipo o hacer que sus datos sean vulnerables a ataques de piratas informáticos, hay muchas aplicaciones inofensivas que se detectan como programas espía durante un análisis. Si utiliza algunas de estas aplicaciones, por ejemplo, un software de reconocimiento de voz, puede agregarla a la lista de excepciones para excluirla de los análisis de programas espía. Para agregar programas espía a la lista de excepciones, haga clic con el botón derecho en el elemento correspondiente de la lista Resultados del análisis y seleccione la opción de menú Ignorar siempre.

Resultados del análisis de virus y programas espía

El cuadro de diálogo Resultados del análisis, que muestra los resultados de los análisis de virus y programas espía, ahora incluye el área Detalles. Para los análisis de programas espía, el área Detalles muestra las rutas completas de todos los rastros de programas espía (como claves de registro, cookies, etc.). Esta información puede resultar útil para usuarios avanzados que deseen realizar un seguimiento de los programas espía que el software de seguridad de Zone Alarm no trate automáticamente. Para los resultados de los análisis de virus, el área Detalles permanece vacía.

Control de componentes

La documentación se ha actualizado para describir de una forma más precisa la interacción entre el control de programas y el control de componentes. A continuación se incluye el texto actualizado:

Independientemente de la configuración del control de programas, el control de componentes estará desactivado de forma predeterminada. Aunque se cambie el nivel de control de programas, no se activará automáticamente el control de componentes. Sin embargo, si activa el control de componentes, éste permanecerá activado mientras que el control de programas esté establecido en Alto, Medio o Bajo.

Nuevo comportamiento para Recordar esta configuración

La versión 6.5 incluye un nuevo comportamiento para la casilla de verificación **Recordar esta configuración** en las alertas de programas. Ésta es la nueva descripción:

Mientras SmartDefense Advisor esté configurado como Automático, el software de seguridad de Zone Labs mostrará las alertas de programas únicamente si no hay ninguna configuración automática disponible. Si selecciona la opción **Recordar esta configuración** en una alerta de programa al permitir o denegar el acceso de un programa, el software de seguridad de Zone Labs conservará su configuración a menos que SmartDefense Advisor disponga de una configuración diferente o hasta que cambie la configuración manualmente en la ficha Programas. Si no selecciona **Recordar esta configuración**, el software de seguridad de Zone Labs mostrará otra alerta de programa la próxima vez que el programa intente la misma acción.

Cambio de nombre en el panel Servidor de seguridad

Ha cambiado el nombre de una de las opciones de seguridad de la zona de Internet y de la zona de confianza, que se encuentran en la ficha Principal del panel Servidor de seguridad. La opción Bajo ahora se llama Desactivado.

Nuevos iconos de la barra de tareas

La versión 6.5 incluye los siguientes iconos nuevos:

Icono	Descripción
	El software de seguridad de Zone Alarm está realizando un análisis de virus y/o programas espía. Si desea obtener información detallada sobre los análisis de programas espía, consulte la ayuda en línea asociada y las secciones sobre programas espía que se incluyen en "Actualizaciones y correcciones de documentación", en la página 8 de este documento. Cuando este icono esté visible, haga clic en él con el botón derecho y seleccione **Ver análisis** para acceder al cuadro de diálogo Estado del análisis.
	El modo de juego está activado, lo que hace que el software de seguridad de Zone Alarm suprima las actualizaciones, los análisis y la mayoría de las alertas. Si desea obtener información detallada sobre el modo de juego, consulte "Modo de juego", en la página 2.
	El software de seguridad de Zone Alarm está recibiendo una actualización, como una actualización de nuevas definiciones de virus o de programas espía.